UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/752,134	12/27/2000	Gilbert Neiger	042392.P9770	8719

8791 7590 10/21/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
SCHUBERT, KEVIN R	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 10/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/752,134	NEIGER ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *see attached*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-30 have been considered.

Specification

A reference error occurs in the fifth sentence of the eighth paragraph of the Description of Embodiments. The applicant refers to "VMs 102 and 112" while the VMs in Figure 1 are identified as 102 and 114. The examiner will assume applicant meant to write VMs 102 and 114. Appropriate correction is required.

A reference error occurs in the fifth sentence of the ninth paragraph of the Description of Embodiments. The applicant refers to "guest applications 206" while the guest applications in Figure 2 are designated as 204. The examiner will assume applicant meant to write guest applications 204. Appropriate correction is required.

Claim Objections

Claim 21 is objected to because of the following informalities: "reporting" should be "report". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 9 and 23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention. The applicant discloses a method of determining that the attempt of the guest software is potentially successful, but it is not clear in the determination step what the actual result of a "potentially successful" attempt would be or to what degree "potentially" refers to. Proper clarification is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-8,15-22,28,29 are rejected under 35 U.S.C. 102(e) as being anticipated by Lim, U.S. Patent No. 6,795,966.

As per claims 1 and 28, the applicant discloses the following method which is anticipated by Lim:

a) running guest software in a processor mode that enables the guest software to operate at a privilege level intended by the guest software (column 14, lines 28-40);

b) responsive to an attempt of the guest software to perform an operation restricted by said processor mode, exiting said processor mode to transfer control over the operation to the VMM running outside said processor mode (column 6, lines 45-52; column 29, lines 15-20);

The applicant should note that the guest software of part a) is referred to as applications 220 by Lim and that these applications run "normally". Applicant should also note that Lim discloses that the process whereby a checkpoint is initiated can be automated as given in the example of virus protection. Therefore, an attempt by the processor to perform an operation which should come after the checkpoint can be deemed restricted by the processor, so part b) is satisfied by Lim.

As per claims 2,16, and 29, the applicant discloses the independent claim, which is satisfied by Lim (see above), with the following limitation which is also satisfied by Lim:

a) responding to the operation (column 6, lines 53-65);

b) transferring control over the operation to the guest software by entering said processor mode (column 6, lines 53-65);

As per claims 3 and 17, the applicant discloses the independent claim, which is satisfied by Lim (see above), with the following limitation which is also satisfied by Lim:

wherein entering said processor mode includes loading processor state expected by the guest software (column 6, lines 53-65);

As per claims 4 and 18, the applicant discloses the independent claim, which is satisfied by Lim (see above), with the following limitation which is also satisfied by Lim:

a) saving processor state used by the guest software (column 6, lines 53-65);

b) loading processor state required by the VMM (column 10, lines 32-38);

As per claims 5 and 19, the applicant discloses the independent claim, which is satisfied by Lim (see above), with the following limitation which is also satisfied by Lim:

wherein exiting said processor mode further comprises automatically transferring from an address space associated with the guest software to an address space associated with the VMM (column 29, lines 39-42);

The applicant should also note the diagram in Figure 2 whereby the dually pointed arrow which connects VM 200 with VMM 250 represents the flow of data which occurs from an address space associated with a VM to the address space associated with the VMM.

As per claims 6 and 20, the applicant discloses the independent claim, which is satisfied by Lim (see above), with the following limitation which is also satisfied by Lim:

maintaining a flag in a processor control register to indicate whether the processor is in said processor mode (column 10, lines 9-23);

The applicant should note that Lim discloses that flags, pointers, and tables are stored in registers in order to enable the processor to load the correct current memory segment. Indicating whether the processor is in said processor mode would be one aspect of the register flags.

As per claims 7 and 21, the applicant discloses the independent claim, which is satisfied by Lim (see above), with the following limitation which is also satisfied by Lim:

reporting an ability of a processor to support said processor mode using one of a plurality of reserved feature bits that are returned in a processor register (column 29, lines 50-57);

As per claims 8 and 22, the applicant discloses the independent claim, which is satisfied by Lim (see above), with the following limitation which is also satisfied by Lim:

wherein exiting said processor mode comprises generating one of a plurality of interrupts and exceptions in response to the attempt of the guest software to perform the operation restricted by said processor mode (column 26, lines 32-40; column 29, lines 15-20);

Similar to claim 1, applicant should note that Lim discloses that the process whereby a checkpoint is initiated can be automated as given in the example of virus protection. Therefore, an attempt by the processor to perform an operation which should come after the checkpoint can be deemed restricted by the processor.

As per claim 15, the applicant discloses the system with the limitations of claim 1, which is satisfied by Lim (see above), that has the additional component of a memory which is also satisfied by Lim (column 14, lines 28-33).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims10-14,24-27, and 30 are rejected under 35 U.S.C. 103(a).

Claims 11-12,14, and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lim in further view of Rozycki (Rozycki, Maciej W. Protected Mode Virtual Interrupts (PVI) on Pentium and SL-enhanced i486 Intel processors. 1996).

Claims 10,24, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Lim in further view of Rozycki in further view of Collins (Collins, Robert R. Details of Intel's Virtual Mode Extensions (VME)). Claims 13 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lim in further view of Rozycki in further view of Walker (Walker, Wade and Cragon, Harvey. Interrupt Processing in Concurrent Processors. June 1995. Computer. pp. 36-46).

As per claims 11 and 25, the applicant further limits claim 8 and 22, respectively, with the following:

a) identifying an attempt of the guest software to modify an interrupt flag (page 1);

b) modifying the interrupt flag if the interrupt flag does not control masking of interrupts (page 3);

Lim discloses everything as applied to claims 8 and 22 (see above). However, Lim fails to specifically teach a) and b) above. Rozycki teaches identifying an attempt of guest software to modify an interrupt flag: "To ensure protection and accessibility at the same time, a special two-bit field called IOPL was introduced into the EFLAGS register... In this way, disabling of access to these instructions can be achieved. Additionally, to prevent user-level code from changing the IOPL field, POPF or IRET do not modify it when executed at CPL > 0" (page 1, paragraph 2). Thus, in order to prevent the user from making modifications, there is a step of identifying a user or guest attempt to make modifications.

Furthermore, Rozycki teaches modifying the interrupt flag if the interrupt flag does not control masking of interrupts. Rozycki discloses a technique whereby a flag is checked and based upon its value appropriate action is taken and where it is possible to execute some system level programs or procedures at the application level. Such is the

scenario described by the applicant in the thirty-fourth paragraph of the Description of Embodiments whereby a flag is checked and based upon its value appropriate action is taken to modify or not modify the flag.

As described by Rozycki in the Introduction, identifying attempts of the guest to modify interrupt flags and modifying interrupt flags if they do not control masking are good ways to ensure protection and accessibility at the same time. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to have combined Rozycki with Lim in order to make Lim's system more protected and robust.

As per claims 12 and 26, the applicant further limits claim 8 and 22, respectively, with the following:

a) identifying an attempt of the guest software to modify an interrupt flag (page 1);

b) preventing the attempt of the guest software to modify the interrupt flag (pages 2 and 3);

Lim discloses everything as applied to claims 8 and 22 (see above). However, Lim fails to specifically teach a) and b) above. Rozycki teaches identifying an attempt of guest software to modify an interrupt flag: "To ensure protection and accessibility at the same time, a special two-bit field called IOPL was introduced into the EFLAGS register... In this way, disabling of access to these instructions can be achieved. Additionally, to prevent user-level code from changing the IOPL field, POPF or IRET do not modify it when executed at CPL > 0." Thus, in order to prevent the user from making modifications, there is a step of identifying a user or guest attempt to make modifications.

Furthermore, Rozycki teaches preventing the attempt of the guest software to modify the interrupt flag. Rozycki says on page 2, "The OS may detect executing of the CLI or STI instruction and set appropriate internal variables that would decide whether to let the application serve the interrupt or not". Rozycki also describes a number of conditions on the bottom of page 2 and the top of page 3 which prevent the user or guest from manipulating interrupt flags. These conditions could be set so that interrupt flags are never modified by the guest software or user.

As described by Rozycki in the Introduction, identifying attempts of the guest to modify interrupt flags and preventing the guest from modifying the interrupt flags are good ways to ensure protection and accessibility at the same time. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to have combined Rozycki with Lim in order to make Lim's system more protected and robust.

As per claim 14, the applicant further limits claim 12 with the following limitation which is met by Rozycki:

wherein preventing the attempt of the guest software to modify the interrupt flag includes generating one of the plurality of interrupts and exceptions in response to the attempt of the guest software to modify the interrupt flag (page 2);

The combination of Lim and Rozycki discloses all the limits of claim 12 (see above). Lim fails to specify that guest attempts at modifying the interrupt flag generate one of a plurality of interrupts and exceptions. Rozycki discloses that a General Protection Fault exception will occur if the user-level or guest software tries to execute any instructions when the current privilege level (CPL) is greater than the input/output privilege level (IOPL).

It would have been an obvious improvement over Lim to one of ordinary skill in the art at the time the invention was filed to add the generation of interrupts and exceptions in response to the attempt of the guest software to modify the interrupt flag because the interrupts and exceptions would add an additional security function to Lim's system.

As per claims 10,24, and 30 the applicant further limits claims 8,22, and 28, respectively, with the following limitation which is met by Collins:

a) maintaining a redirection bitmap for the plurality of the interrupts and exception, the redirection bitmap indicating whether each of the plurality of the interrupts and exceptions is allowed to be handled by the guest software (page 3);

b) consulting the redirection bitmap to determine whether to exit said processor mode (page 7);

Lim and Rozycki meet all the limitations of claims 10,24, and 30. They fail to teach maintaining a redirection bitmap and consulting a redirection bitmap to determine whether to exit the processor mode. Describing the benefits of using a redirection bitmap, Collins writes, "Memory managers can primarily benefit by the use of the interrupt redirection bitmap to reduce the number of switches to and from protected mode. This has the added benefit of reducing the complexity of the interrupt service routines, as they no longer need to reflect software interrupts back to the v86 task." In order to reduce the complexity of switches to and from the processor mode, it would have been obvious to one of ordinary skill in the art at the time the invention was filed to have added a redirection bitmap to the teachings of Lim and Rozycki.

As per claims 13 and 27, the applicant further limits claims 12 and 26, respectively, with the following limitation which is met by Walker:

wherein preventing the attempt of the guest software to modify the interrupt flag includes providing a shadow interrupt flag for modifications by the guest software (page 7);

Lim and Rozycki meet all the limitations of claims 12 and 26 (see above). Lim and Rozycki fail to teach the use of shadow flags to prevent the attempt of guest software to modify the interrupt flag. Walker discloses that the use of shadow registers is a good way to further limit the manipulation of the actual registers because the original state of the actual register is maintained while the shadow state is being manipulated. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to have combined the ideas of Walker with those of Lim and Rozycki to produce a system which has shadow flags to further limit the manipulation of actual flags.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

Andrew Caldwell

Andrew Caldwell